Enterprise Standards and Approved Products

August 2008

5000 Security Domain

Category	Enterprise Standard (Web Site Links are located at end of document)	Product(s) (Web Site Links are located at end of document)	Effective Date
5010 Intrusion Detection and Prevention	Products must support approved Enterprise standards in the following categories: ▪ Operating systems—specific Unix operating systems (OSs), MS Windows ▪ Network topologies—Ethernet, T1/E1 ▪ Switched networks ▪ Protocols—TCP/IP, UDP ▪ Applications—FTP, HTTP, Telnet ▪ Firewalls Products should be OBDC-compliant for links to EAS-approved databases.	**Top Layer Products:** ▪ Nortel SourceFire ▪ ISS Proventia ▪ McAfee Host IPS **Internet Security Systems Products:** ▪ RealSecure Network Protection ▪ RealSecure Server Sensor ▪ RealSecure Site Protector ▪ Symantec Deepsight	Revision date: Aug 21, 2008 Effective date: June 1, 2003
5100 Encryption	**IETF X.509 Public Key Infrastructure** (PKI latest version for digital certificates) Interoperates and fully supports critical enterprise infrastructure services and applications such as network protocols, desktop operating systems, e-mail, web servers, database management software, firewalls and directory services. Symmetric encryption algorithms required for securing content: U.S. Data Encryption Standard (DES) in accordance with U.S. FIPS PUB 46-2 and ANSI X3.92 and Triple-DES in accordance with ANSI X9.52	**Entrust** suite of PKI enabled products for digital signature technology and securing e-mail transport of content and attachments.	Revision date: December 1, 2008 Effective date: July 1, 1997

Category	Enterprise Standard (Web Site Links are located at end of document)	Product(s) (Web Site Links are located at end of document)	Effective Date
5505 Sanitization and Disposal of Information Technology Equipment and Electronic Media	The recognized authority for Sanitization and Disposal standards are the **National Institute of Standards and Technology** referenced in their documents: ▪ Guidelines for Media Sanitization ▪ Guide to Selecting Information Technology Security Products, Section 5.9 And U.S. Department of Defense Standard: DoD 5220.22-M: *National Industrial Security Program Operating Manual (NISPOM)* Archiving Records: Any IT devices (servers, storage, clients), network components, operating system or application software, or storage media containing public records as defined by KRS 61.870(2) and 171.410 shall have the final disposition of those records established with the Kentucky Department for Libraries and Archives prior to disposal through the Division of Surplus Property (Finance) or transfer to other agencies for re-use**.** CIO-077, Sanitization of IT Equipment: This enterprise policy provides detailed information relating to DoD requirements and their implementation. Physical Destruction: Physical destruction is an acceptable option for devices and portable media that are permanently being disposed. On storage devices or media that have been rendered inoperable because of failure, physical destruction is required. See the Technical and Implementation Considerations section for more details on this option. **Note:** Effective February 7, 2003, the Division of Surplus Property will not accept computers for surplus without a statement that the device has been sanitized in accordance with CIO-077.	Approved products and mechanisms for rendering data inaccessible depend on the type of media being used and the disposition of the device or media. Further discussion is provided under Technical and Implementation Considerations. Recommended Products: Disks: **WipeDrive**: Files: **SecureClean**	Revision date: Aug 21, 2008 Effective date: February 14, 2003

Category	Enterprise Standard (Web Site Links are located at end of document)	Product(s) (Web Site Links are located at end of document)	Effective Date
5515 Secure Transport	Secure Socket Layer (SSL) 3.0 encryption (minimum 40-bit) is required if data needs to be secured via the Internet. All electronic payments (credit card, EFT, etc) and the collection of personally identifiable information must be secured during transport (see Category 3505 Network Services - Electronic Commerce and Payments). Strong encryption (128-bit) is recommended and may be required for certain applications, particularly personal and health-related information as prescribed in federal law. To authenticate and secure the web server, a server certificate (digital ID), available from Entrust, must assigned to the web server. This includes secure servers operated under contract, although any server certificate software may be used in those instances. See Category 3510 Network Services - Internet/Intranet Web Server. Secure Shell (SSH) is a Unix-based command interface and protocol for securely accessing a remote computer. This protocol can be used for remote access, such as telnet, as well as secure data transport through SFTP. Current SSH standards support Blowfish, DES, and IDEA encryption algorithms.	**Entrust.net** Secure Socket Layer (SSL) server certificates Both web browser approved products (**Category 3511**) support SSL 3.0 Both web server approved products (**Category 3510**) support SSL 3.0 Secure Shell (SSH), Secure Shell v2 (SSH2)	Revision date: Aug 21, 2008 Effective date: June 1, 1999
5530 Virus Scanning	Support for all approved hardware platforms, operating systems software and applications. Ability to detect an infected file at the server and desktop level, with regular updates of the virus definition files.	Windows Server OS: ▪ **McAfee Active Virus Defense** (Network Associates) Windows Desktop OS: ▪ **VirusScan by McAfee** (Network Associates) ▪ **McAfee Total Protection for Small Business** (Network Associates) Linux OS: ▪ **McAfee LinuxShield** (Network Associates) Microsoft Exchange: ▪ **McAfee GroupShield** (Network Associates) Microsoft Sharepoint ▪ **Microsoft ForeFront Security** NetWare ▪ **McAfee NetShield for NetWare** (Network Associates)	Revision date: Aug 21, 2008 Effective date: July 1, 1997
5545 Spam Filtering	Support for all approved hardware platforms, operating systems software and applications. Ability to detect an unsolicited or inappropriate email and deliver to a separate inbox for review before delivery to the addressee.	**Ironmail** (Secure Computing)	Effective Date: Aug 21, 2008

Category	Enterprise Standard (Web Site Links are located at end of document)	Product(s) (Web Site Links are located at end of document)	Effective Date
5700 Firewall	▪ International Computer Security Association (ICSA) - ICSA Labs® Certification for firewall products ▪ Firewall Product Developers Consortium (FWPD) Product Certification Criteria ▪ Internet Protocol Security Protocol Working Group (IPsec), part of the Internet Engineering Task Force (IETF) ▪ National Institute of Standards and Technology (NIST) Firewall Protection Profile ▪ Support all Internet Protocol (IP) stacks ▪ Approved application servers and operating system (OS) ▪ Integration with internetworking hardware and software from Nortel Networks Based on the enterprise policy CIO-076, COT shall manage all enterprise and intranet firewall and VPN services that utilize the KIH infrastructure. Agencies may manage agency-level Tier II firewall services under certain stipulations and with COT network visibility to the firewall. It is imperative that network services for all agencies within the KIH are protected and that the integrity of the KIH is protected to insure that enterprise services are not compromised. The administration of firewalls and virtual private networks (VPN) is a critical component in securing the KIH infrastructure and computing systems. ▪ Internet and Extranet (business relationships) VPN connections must be managed to maintain enterprise security and reduce security risks. For this reason, COT shall be the approving authority for access to KIH computing resources. Agencies using the Internet to communicate and share data must use the COT-managed VPN service. ▪ Intranet VPN connections shall be managed by COT to maintain enterprise security and network routing efficiencies. Agencies wanting to create Intranet VPN's must use COT VPN approved services.	**Check Point Firewall-1** is the approved product standard for Tier I firewall services. Tier I classification includes all services and/or systems that are considered an enterprise resource. Enterprise resources should be located at the Commonwealth's Data Center (CDC) in order to maximize security benefits and network efficiency. Enterprise resources located at CDC benefit from additional security technologies in place there. **Nortel Networks Contivity** firewall product is the enterprise standard for Tier II firewall services. Tier II classification includes all services and/or systems that are agency-specific but available for the enterprise. Agency-specific applications and services would be suitable for Tier II firewall services. Tier II firewall services may not be interoperable with other enterprise security platforms. NOTE: Agencies are encouraged to review the COT security offering for firewall services.	Revision Date: Aug 21, 2008 Effective date: July 1, 1997
5710 Desktop/Laptop Firewall Software	▪ All state-owned laptop computers must have desktop/laptop firewall software installed on them. ▪ All VPN-connected and dial-up connected workstations that remotely connect to the state's network must have desktop/laptop firewall software installed on them.	The current approved and supported enterprise standards for individual computers connecting to the Commonwealth's Intranet are: ▪ **Microsoft Windows Firewall** ▪ Network Associates Inc. (NAI) **- McAfee Personal Firewall Plus** ▪ **McAfee HIPS** ▪ **Netmotion** ▪ **Symantec - Norton Personal Firewall** ▪ **Zone Labs: Zone Alarm** (free for home use); **Zone Alarm Plus**; **Zone Alarm Pro**; Zone Labs' enterprise solution includes **Zone Labs Integrity**, **Zone Labs Integrity Desktop**, and **Integrity Desktop Manager** (simple deployment tool).	Revision date: Aug 21, 2008 Effective date: December 5, 2003

Web Site Links:

External Links: Some of the following links resolve to non-governmental agencies. The information on these pages is not controlled by COT or the Commonwealth of KY.

Category:	Link:	URL:
5515	Category 3510	http://gotsource.ky.gov/docushare/dsweb/Get/Document-301105/
5515	Category 3511	http://gotsource.ky.gov/docushare/dsweb/Get/Document-301105/
5700	Check Point Firewall-1	http://www.checkpoint.com/products/softwareblades/firewall.html
5700	CIO-076	http://www.gotsource.net/docushare/dsweb/Get/Document-13776/
5505	CIO-077	http://gotsource.ky.gov/docushare/dsweb/Get/Document-17661/
5505	DoD 5220.22-M: National Industrial Security Program Operating Manual (NISPOM)	https://www.dss.mil/GW/portlets/AutonomyRetrieval/autosuggest.jsp?username=e8e9e6e5f9e0f8&threshold=20&numresult=10&defaultlogo=i_html.gif&display=782&url=%2Fusr%2Flocal%2Fweblogic%2Fbea92%2FportalContent%2F%2Fisp%2Fodaa%2Fdocuments%2Fnispom2006-5220.pdf&links=DOD,522022,M&command=getoriginal
5100	Entrust suite	http://www.entrust.com/
5515	Entrust.net	http://www.entrust.net/
5700	Firewall Product Developers Consortium (FWPD) Product Certification Criteria	http://www.icsalabs.com/icsa/topic.php?tid=jgjgjg$dsf-sfddf
5505	Guide to Selecting Information Technology Security Products, Section 5.9	http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
5505	Guidelines for Media Sanitization	http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
5100	IETF X.509 Public Key Infrastructure	http://www.ietf.org/
5700	International Computer Security Association (ICSA)	http://www.icsalabs.com/icsa/icsahome.php
5700	Internet Protocol Security Protocol Working Group (IPsec)	http://technet.microsoft.com/en-us/network/bb531150.aspx
5545	Ironmail	http://www.securecomputing.com/index.cfm?skey=1612
5010	ISS Proventia	http://www-935.ibm.com/services/us/index.wss/offering/iss/a1027756
5530	McAfee Active Virus Defense	http://www.mcafee.com/us/enterprise/products/security_suite_solutions/active_virus_defense.html
5530	McAfee GroupShield	http://www.mcafee.com/us/enterprise/products/anti_virus/email_servers/groupshield_microsoft_exchange.html
5010, 5710	McAfee Host IPS	http://www.mcafee.com/us/enterprise/services/product_training/host_based_intrusion_protection_system.html
5530	McAfee LinuxShield	http://www.mcafee.com/us/enterprise/products/system_security/servers/linuxshield.html
5530	McAfee NetShield for NetWare	http://www.mcafee.com/us/enterprise/products/anti_virus/file_servers_desktops/netshield_netware.html
5710	McAfee Personal Firewall Plus	http://download.mcafee.com/products/manuals/en-us/MPF_DataSheet_2006.pdf
5530	McAfee Total Protection for Small Business	http://www.mcafee.com/sg/small/products/security_compliance_services/total_protection_service.html
5530	Microsoft ForeFront Security	http://www.microsoft.com/forefront/en/us/default.aspx

Web Site Links:

External Links: Some of the following links resolve to non-governmental agencies. The information on these pages is not controlled by COT or the Commonwealth of KY.

Category:	Link:	URL:
5710	Microsoft Windows Firewall	http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx
5505, 5700	National Institute of Standards and Technology	http://www.nist.gov/index.html
5710	Netmotion	http://www.netmotionwireless.com/
5700	Nortel Networks	http://www.nortel.com/
5010	Nortel SourceFire	http://www.sourcefire.com/partners/technology
5010	RealSecure (Network Protection, Server Sensor, Site Protector)	http://www-935.ibm.com/services/us/index.wss/offerfamily/iss/a1029097
5505	SecureClean	http://www.whitecanyon.com/secureclean-clean-hard-drive.php?gclid=CJKloYvfzZkCFRKLxwodLjP2ug
5710	Symantec - Norton	http://www.symantec.com/index.jsp
5530	VirusScan by McAfee	http://www.mcafee.com/us/enterprise/products/anti_virus/file_servers_desktops/virusscan_enterprise_80i.html
5505	WipeDrive	http://www.accessdata.com/products.html
5710	Zone Labs	http://www.zonealarm.com/security/en-us/home.htm?lid=en-us